

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09218852 A**(43) Date of publication of application: **19.08.97**

(51) Int. Cl. **G06F 15/00**
G06F 1/00
G06F 13/00
G06F 13/00

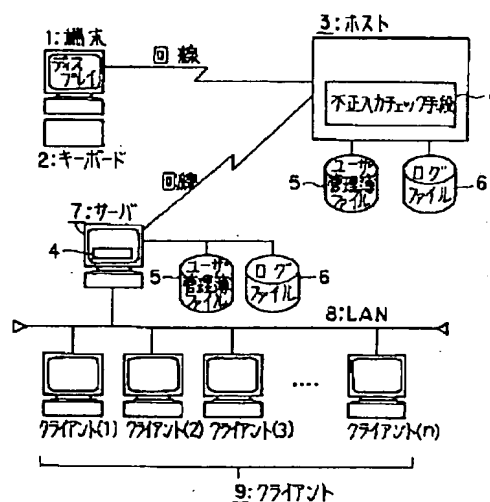
(21) Application number: **08025456**(71) Applicant: **FUJITSU F I P KK**(22) Date of filing: **13.02.96**(72) Inventor: **FUKUI TAKAMITSU**(54) **ILLEGALITY CHECKING SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized use by reporting unauthorized access and an unauthorized character string to a normal user and making him/her change a password or the like.

SOLUTION: This system is provided with an unauthorized input checking means for retrieving a user management book 5 corresponding to the input of a user ID through a line, urging the input of the password when it is registered, repeating the storage of the inputted character string and the date and time of the input in a log file 6 and the urging of re-input when the inputted character string is not correct for the password registered corresponding to the user ID of the user management book 5, performing disconnection in exceeding the prescribed number of times, and on the other hand, when it is correct, connecting the line, displaying the previously stored incorrect unauthorized character string, date and time inside the log file 6 and displaying the log-out date and time of a previous time.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-218852

(43) 公開日 平成9年(1997)8月19日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0		G 0 6 F 15/00	3 3 0 B
1/00	3 7 0		1/00	3 7 0 E
13/00	3 5 1		13/00	3 5 1 F
	3 5 7			3 5 7 Z

審査請求 未請求 請求項の数 4 O L (全 9 頁)

(21) 出願番号 特願平8-25456

(22) 出願日 平成8年(1996)2月13日

(71) 出願人 591106864

富士通エフ・アイ・ピー株式会社

東京都港区新橋5丁目36番11号

(72) 発明者 福井 孝光

東京都港区新橋5丁目36番11号 富士通エ

フ・アイ・ピー株式会社内

(74) 代理人 弁理士 岡田 守弘

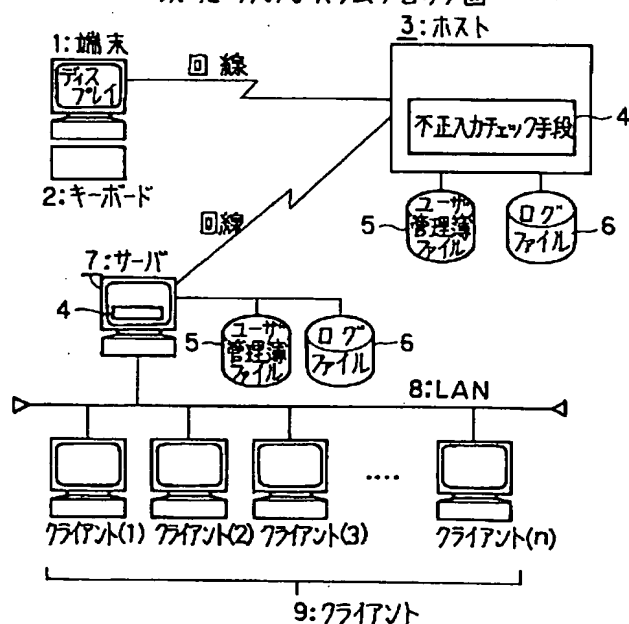
(54) 【発明の名称】 不正チェックシステム

(57) 【要約】

【課題】 本発明は、不正チェックシステムに関し、正規の利用者に不正アクセスおよび不正文字列を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることを目的とする。

【解決手段】 回線を介した利用者IDの入力に対応してユーザ管理簿を検索して登録されているときに暗証番号の入力を促し、入力された文字列がユーザ管理簿の利用者IDに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えるように構成する。

本発明のシステムブロック図



【特許請求の範囲】

【請求項1】回線を介したログインの不正チェックを行う不正チェックシステムにおいて、

利用者IDに対応づけて暗証番号を登録するユーザ管理簿と、

回線を介した利用者IDの入力に対応して上記ユーザ管理簿を検索して登録されているときに暗証番号の入力を促し、入力された文字列が上記ユーザ管理簿の上記利用者IDに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えたことを特徴とする不正チェックシステム。

【請求項2】回線を介したログインの不正チェックを行う不正チェックシステムにおいて、

利用者IDと暗証番号とを対応づけて登録するユーザ管理簿と、

回線を介した利用者IDおよび暗証番号の入力に対応して上記ユーザ管理簿を検索して利用者IDに対する暗証番号が正しくないときに入力を促し、入力された文字列が上記ユーザ管理簿の上記利用者IDに対する暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示する不正入力チェック手段とを備えたことを特徴とする不正チェックシステム。

【請求項3】上記正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時の表示を、当該正しいときに回線接続の回数が所定回数を越えるまで繰り返し表示、あるいは当該正しいときに回線接続の日から所定日以前までのものを表示することを特徴とする請求項1あるいは請求項2記載の不正チェックシステム。

【請求項4】上記不正ログイン後あるいは不正ログインが所定回数越えたときに、所定期間の間、該当する利用者IDのログインを許可しないことを特徴とする請求項1ないし請求項3記載のいずれかの不正チェックシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、回線を介したログインの不正チェックを行う不正チェックシステムに関するものである。

【0002】

【従来の技術】従来、パソコン通信などでは、ログイン

時に、「前回のログアウト日時」を下記のように表示し、第三者が本人になりすました利用がないかをチェックすることを行っていた。

【0003】前回LOG OUT 95/09/10 10:11:12

【0004】

【発明が解決しようとする課題】しかし、ログイン時に前回のログアウト日時が表示されても、第三者に不正使用されたかをチェックするには、自分の前回のログアウト日時を記憶してそれと比較して自分がアクセスした日時か、他人が不正にアクセスした日時かを判別する必要があり、確認が行い難いという問題があった。

【0005】また、不正の第三者が他人の暗証番号を知るために、その本人の利用者番号（ID）を入力し、その後、想定した暗証番号（パスワード）を入力してトライしても、通常は数回のトライで正しくないので通信が途絶（切断）される。しかし、再度異なる想定される暗証番号を入力してトライすることを繰り返しても、その不正トライの事実を本人が知ることができなかった。このために、他人の利用者番号（ID）に対して何度も暗証番号を入力してトライし、その暗証番号を探りだし、不正利用を許すことになってしまうという問題があった。

【0006】また、金融機関では、第三者が不正利用の目的で、不正なパスワードが投入された場合、所定の回数を越えたときにカードなどを無効にし、再使用できないようにしてしまうため、度忘れしたり間違いして間違ったパスワードを繰り返し入力してしまった正規の利用者が利用できなくなる問題もあった。この際、パソコン通信などでは、不正利用を完全に無くすよりも、不正利用のトライがあったことを正規利用者に知らせたり、不正利用から守るようにしたりする工夫が望まれている。

【0007】本発明は、これらの問題を解決するために、回線を介して入力された利用者IDおよび暗証番号について間違った入力があったときに所定回数のリトライを許すと共に不正アクセスを記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示し、正規の利用者に不正アクセスおよび不正文字列を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることを目的としている。

【0008】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、ホスト4は、端末1やサーバ7に接続して各種サービスを提供するものであって、ここでは、不正入力チェック手段4などから構成されるものである。

【0009】不正入力チェック手段4は、ユーザ管理簿5を参照してログイン時の不正をチェックしたり、チェックして不正と判明したときに入力された文字列、日時などのログをログファイル6に格納したり、正常なログイン時に過去の不正な文字列、日時などを表示したりな

とするものである。

【0010】サーバ7は、LAN8に接続されたクライアントを統括管理するものであって、ここでは、不正入力チェック手段4などから構成されるものである。ユーザ管理簿ファイル5は、利用者IDに対応づけて暗証番号を管理するものである。

【0011】ログファイル6は、不正ログイン時に入力された文字列、日時などを保存するものである。次に、動作を説明する。

【0012】不正入力チェック手段4が回線を介した利用者IDの入力に対応してユーザ管理簿ファイル5を検索して登録されているときに暗証番号の入力を促し、入力された文字列がユーザ管理簿ファイル5の利用者IDに対応づけて登録されている暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル6内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示するようにしている。

【0013】また、不正入力チェック手段4が回線を介した利用者IDおよび暗証番号の入力に対応してユーザ管理簿ファイル5を検索して利用者IDに対する暗証番号が正しくないときに入力を促し、入力された文字列がユーザ管理簿ファイル5の利用者IDに対する暗証番号に正しくないときに入力された文字列と入力された日時をログファイルに格納および再入力を促すことを繰り返し、所定回数越えたときに切断し、一方、正しいときに回線接続して以前に格納したログファイル6内の正しくない不正の文字列と日時を表示および前回のログアウト日時を表示するようにしている。

【0014】これらの際に、正しいときに回線接続して以前に格納したログファイル内の正しくない不正の文字列と日時の表示を、正しいときに回線接続の回数が所定回数を越えるまで繰り返し表示、あるいは正しいときに回線接続の日から所定日以前までのものを表示するようにしている。

【0015】また、不正ログイン後あるいは不正ログインが所定回数越えたときに、所定期間の間、該当する利用者IDのログインを許可しないようにしている。従って、回線を介して入力された利用者IDおよび暗証番号について間違えた入力があったときに所定回数のリトライを許すと共に不正アクセス時の文字列と日時などを不正アクセスログとして記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示することにより、正規の利用者に不正アクセスのあった旨を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることが可能となる。

【0016】

【発明の実施の形態】次に、図1から図5を用いて本発

明の実施の形態および動作を順次詳細に説明する。

【0017】図1は、本発明のシステム構成図を示す。図1において、端末1は、回線を介してホスト4と接続し、各種業務処理を行うものであって、ここでは、ディスプレイ、キーボード2、処理装置などから構成されるものである。

【0018】ホスト4は、回線を介して端末1およびサーバ7と接続し、各種サービスを提供するものであって、ここでは、不正入力チェック手段4などから構成されるものである。

【0019】不正入力チェック手段4は、端末1やクライアント9などから回線を介して利用者IDおよび暗証番号が入力があったときにユーザ管理簿5を参照してログインの不正をチェックしたり、チェックして不正と判明したときに入力された文字列、日時などのログをログファイル6に格納したり、正常なログイン時に過去の不正なログインされた文字列、日時などを表示したりなどするものである。

【0020】ユーザ管理簿ファイル5は、利用者IDと暗証番号とを対応づけて管理するものである（図3参照）。ログファイル6は、不正ログイン時に入力された文字列、日時などを保存するものである（図3参照）。

【0021】サーバ7は、LAN8を介して複数のクライアント9を統括制御および回線を介してホスト3に接続したりなどするものであって、ここでは、不正入力チェック手段4などから構成されるものである。

【0022】LAN8は、ローカルエリアネットワークであって、複数のクライアント(1)ないし(n)およびサーバ7を相互に接続するものである。クライアント9は、クライアント(1)ないし(n)から構成され、LAN8を介して相互に接続およびサーバ7に接続、更にサーバ7経由でホスト3に接続し、各種業務処理を行うものである。

【0023】次に、図2のフローチャートに示す順序に従い、図1の構成の動作を詳細に説明する。図2において、S1は、利用者番号(ID)の入力要求を行う。

【0024】S2は、S1の入力要求に応じて、利用者が利用者番号を入力する。これは、例えば図1の端末1から回線を介してホスト3に接続し、端末1のディスプレイ上に表示された利用者番号(ID)の入力フィールドに利用者番号(ID)をキー入力する。

【0025】S3は、ユーザ管理簿ファイルと照合する。これは、S2で入力された利用者番号(ID)を回線を介して受信したホスト3の不正入力チェック手段4がこの受信した利用者番号(ID)が、ユーザ管理簿ファイル5に登録されているか照合する。

【0026】S4は、OKか否かを判別する。YESの場合には、利用者番号(ID)がユーザ管理簿ファイル5に登録されていると判明したので、S8に進む。一方、NOの場合には、利用者番号(ID)がユーザ管理

簿ファイル5に登録されていないと判明したので、S5に進む。

【0027】S5は、エラー回数がn回か判別する。YESの場合には、トライ回数nの制限を越えたと判明したので、S7で切断する。一方、NOの場合には、トライ回数n以内と判明したので、S6で再入力要求を行い、S1以降を繰り返す。

【0028】以上のS1からS7によって、利用者が図1の端末1を使ってホスト4に接続してログインするときに、利用者番号(ID)を入力してユーザ管理簿ファイル5に登録されているか否かを判別し、YESのときにS8以降の処理に進み、NOのときに回線を切断する。

【0029】S8は、パスワード(暗証番号)の入力要求を行う。S9は、S8の入力要求に応じて、利用者がパスワードを入力する。これは、例えば図1の端末1から回線を介してホスト3に接続し、端末1のディスプレイ上に表示されたパスワードの入力フィールドにパスワードをキー入力する。

【0030】S10は、ユーザ管理簿ファイルと照合する。これは、S9で入力されたパスワードを回線を介して受信したホスト3の不正入力チェック手段4がこの受信したパスワードが、ユーザ管理簿ファイル5の利用者番号(ID)に対応づけて登録されているか照合する。

【0031】S11は、OKか否かを判別する。YESの場合には、パスワードがユーザ管理簿ファイル5の利用者番号(ID)に対応づけて登録されていると判明したので、S17に進む。一方、NOの場合には、パスワードがユーザ管理簿ファイル5の利用者番号(ID)に対応づけて登録されていないと判明したので、S15に進む。

【0032】S12は、エラー回数がm回か判別する。YESの場合には、トライ回数mの制限を越えたと判明したので、S15で異常アクセスを記録し、S16で回線切断する。例えば異常アクセスしたパスワードの文字列および日時などをログファイル6に、利用者番号(ID)に対応づけて保存する。一方、S12のNOの場合には、トライ回数m以内と判明したので、S14で再入力要求を行い、S8以降を繰り返す。

【0033】以上のS8からS16によって、利用者が図1の端末1を使ってホスト4に接続してログインするときに、利用者番号(ID)がS4のYESでOKとなったときに、パスワードを入力してユーザ管理簿ファイル5に利用者番号(ID)に対応づけてパスワードが登録されているか否かを判別し、YESのときにS17以降の処理に進み、NOのときに異常アクセス記録をログファイル6に保存した後、回線を切断する。

【0034】S17は、エラー情報ありか判別する。これは、S15の異常アクセス記録がログファイル6に当該利用者番号(ID)に対応づけて保存されているか判

別する。YESの場合には、S18ないしS20の処理を行う。一方、S17のNOの場合には、異常アクセスが保存されていないと判明したので、S21の通常処理へ進む。

【0035】S18は、エラー内容を表示する。これは、S17のYESでエラー情報がログファイル6に保存されていると判明したので、エラー内容を表示、例えば後述する図5に示すように、不正パスワード、日時、文字列などを表示する。

【0036】S19は、エラー表示クリアか判別する。これは、Err_flg_off(エラーフラグがOFF)か判別する。YESの場合には、S20でエラー表示クリアを行い、S21に進む。S19のNOの場合には、S21に進む。

【0037】S21は、通常処理へ進む。これは、正規の利用者が端末1を操作してホスト3に回線を介して接続できたので、利用者が端末1を操作してホスト3からの各種サービスの提供を受ける。

【0038】尚、不正ログイン(利用者IDがOKとなったがパスワードが正しくないこと)が所定期間を越えたときに、所定期間の間、該当する利用者IDのパスワードを入力したログインを許可しないようにし、1つの利用者IDに対するパスワードを繰り返し試して探索する事態を防止するようにしてもよい。

【0039】図3は、本発明のファイル例を示す。図3において、ユーザ管理ファイル5は、利用者のID番号に対応づけてパスワード、異常フラグ(Err_flg)、ログ位置などを登録するものである。ここで、異常フラグが異常があったときにONに設定して正規の利用者がホスト3に接続(ログイン)したときに端末1の画面上にエラー情報(図5参照)を表示するためのものである。異常フラグがOFFのときは端末1の画面上にエラー情報を表示しない。

【0040】ログファイル6は、異常アクセスの情報を保存するものであって、ここでは、図示のように、日単位に1回目、2回目・・・のときの時刻および文字列を登録したものである。ここでは、例えば1994年11月07日の1回目の時刻が12時43分51秒で不正パスワードとして入力された文字列が“T-FUKUI Z”である。以下同様に、図示のように保存する。

【0041】図4は、本発明の動作説明フローチャート(その2)を示す。図4において、S31は、利用者が端末1を操作して回線を介してホスト3に接続する。

【0042】S32は、利用者がID(利用者ID)を入力してホスト3に通知する。S33は、登録済みか判別する。これは、ホスト3の不正入力チェック手段4がS32で通知された利用者IDがユーザ管理簿ファイル5に登録されているか判別する。YESの場合には、利用者IDが登録されていると判明したので、S36に進む。一方、NOの場合には、S34で所定期数以内のリ

トライか判別する。YESの場合には、S32に戻り繰り返す。一方、NOの場合には、S35で切断する。

【0043】以上のS31からS35によって、利用者が端末1から正規の利用者IDを入力し、回線を介してホスト3に通知すると、ホスト3の不正入力チェック手段4がユーザ管理簿ファイル5に登録済みのときにS36のパスワードの入力に進み、一方、登録されていないときにリトライが所定回数を越えたときに回線を切断する。

【0044】S36は、利用者がパスワードを入力する。S37は、正しいか判別する。これは、利用者が図1の端末1を操作してパスワードを入力して回線を介してホスト3の不正入力チェック手段4に通知し、当該不正入力チェック手段4がユーザ管理簿ファイル5の利用者IDに対応づけて登録されているパスワードと一致(正しい)か判別する。YESの場合には、パスワードが正しいと判明したので、S41に進む。一方、NOの場合には、S38に進む。

【0045】S38は、データログする。これは、不正のパスワード、日時などをログファイル6に図3に示すように保存する。S39は、所定回数内か判別する。これは、パスワードの入力が所定回数以内でリトライの制限範囲内か判別する。YESの場合には、S36に戻り、利用者にパスワードの入力を促して入力させることを繰り返す。一方、NOの場合には、S40で回線を切断する。

【0046】以上のS36からS40によって、利用者が端末1から正規のパスワードを入力し、回線を介してホスト3に通知すると、ホスト3の不正入力チェック手段4がユーザ管理簿ファイル5に利用者IDに対応づけてパスワードが登録されていたときにS41に進み、一方、登録されていないときにデータログ(不正パスワードの文字列、日時など)を保存およびリトライが所定回数を越えたときに回線を切断する。

【0047】S41は、不正データが有るか判別する。これは、既述した図3のユーザ管理簿ファイル5中の利用者IDに対応する異常フラグがONであって、ログファイル6中に異常アクセス情報(日時と不正パスワードとして入力された文字列など)が保存されているか判別する。YESの場合には、S42に進む。NOの場合には、S46で通常処理へ進む。

【0048】S42は、不正データありのメッセージを表示する。これは、端末1の画面上に不正データありのメッセージを表示し、正規の利用者に不正データ(不正パスワードとして入力された文字列と日時など)がある旨のメッセージを表示する。

【0049】S43は、詳細表示するか判別する。これは、利用者から詳細表示の指示があったか判別する。YESの場合には、S44に進む。NOの場合には、S46で通常処理へ進む。

【0050】S44は、S43で詳細表示すると判明したので、詳細情報(図3のログファイル6の該当するエントリの内容)を表示する。S45は、ログファイルをクリアする。これは、既述した図3のユーザ管理簿ファイル5中の異常フラグをOFFにし、ログファイルの内容が表示済みを設定する。

【0051】S46は、通常処理へ進む。図5は、本発明の表示例(パスワード入力エラー情報表示例)を示す。これは、図1の端末1の画面上に表示したパスワード入力時のエラー情報の表示例である。以下画面上のデータを順次説明する。

【0052】・第1行目の

>User-ID ---->AAA00001

は、利用者が入力した利用者ID"AAA00001"を表す(図3のユーザ管理簿ファイル5の1行目の利用者ID"AAA00001"に対応してここでは、正しいと判明する。

【0053】・第2行目の

>Password ---->

は、利用者が入力したパスワード(画面上には盗用を考慮して非表示)であって、ここでは、"T-FUKUI"と入力されたとなると、図3のユーザ管理簿ファイル5の1行目の利用者ID"AAA00001"に対応した正しいパスワード"T-FUKUI"が入力されたこととなる。

【0054】①は、前回のLOG OUT時刻を表示し、他人によって不正利用されていないかを、利用者に認識させるためのものである。②は、不正なパスワードの入力があったときに表示されるものであって、ここでは、図示のように、"不正なパスワードが入力された情報があります"というメッセージおよび詳細情報表示(1:する 2:しない)の選択番号を表示したものである。ここでは、"1(する)"を選択している。

【0055】③は、②で"1(する)"を選択したことに対応して、エラー情報の詳細が表示されたものである(図3の正規の利用者IDおよびパスワードに対応づけてログファイル6に保存されているエラー情報の詳細を表示したものである。この詳細情報の表示は、予め指定した所定日数前から現在のものを表示したり、所定日までのものを表示したり、所定回数を越えるまで表示したり、任意に表示する。ここでは、例えば第1行目のように、

・不正パスワードの入力日時"1994年11月07日 12時43分51秒" 不正文字列"T-FUKUI Z"を表示する。

【0056】尚、本実施例では、図2および図4では、利用者IDが入力されてOKとなったときに次にパスワードが入力されてOKとなったときに正常運用へ進み、パスワードが入力されてNGのときに異常アクセス情報をログしたけれども、この順序に限られることなく、利用者が端末1の画面上で利用者IDおよびパスワードの

両者を入力してホスト3に通知し、ユーザ管理簿ファイル5を参照して利用者IDおよびパスワードの正当性をどのような順番で判別するようにしてもよい。

【0057】

【発明の効果】以上説明したように、本発明によれば、回線を介して入力された利用者IDおよび暗証番号について間違えた入力があったときに所定回数のリトライを許すと共に不正アクセス時の文字列と日時などを不正アクセスログとして記憶しておき、正常通信開始時に前回のログアウト日時と共に不正アクセスログを表示する構成を採用しているため、正規の利用者に不正アクセスのあった旨を知らせて暗証番号の変更などをさせ不正利用の未然防止を図ることができる。これらにより、

(1) パソコン通信などにおいて、第三者が不正アクセスしようとしていることを、正規の利用者である本人に通知することができる。

【0058】(2) パソコン通信などにおいて、本人が間違えて本人の利用者IDを入力したり、パスワードを間違えて入力したりしても、銀行のカードのように使用不可に書き替えてしまい、業務ができなくなるという事態の発生を無くすることができる。

【0059】(3) パソコン通信などにおいて、他人が不正アクセスしようとしている事実を正規の本人に知らせたり、その不正アクセスの日単位のアクセス回数や不正アクセス時の文字列のログを表示して知らせたりす

ることができる。

(4) 不正アクセス時の文字列を見た利用者は、盗用しようとしたパスワードの文字列を知り、これから容易に盗用できない文字列のパスワードに定期的に変えたりし、未然にパスワードの盗用による不正アクセスを防止できる。

【図面の簡単な説明】

【図1】本発明のシステムブロック図である。

【図2】本発明の動作説明フローチャート(その1)である。

【図3】本発明のファイル例である。

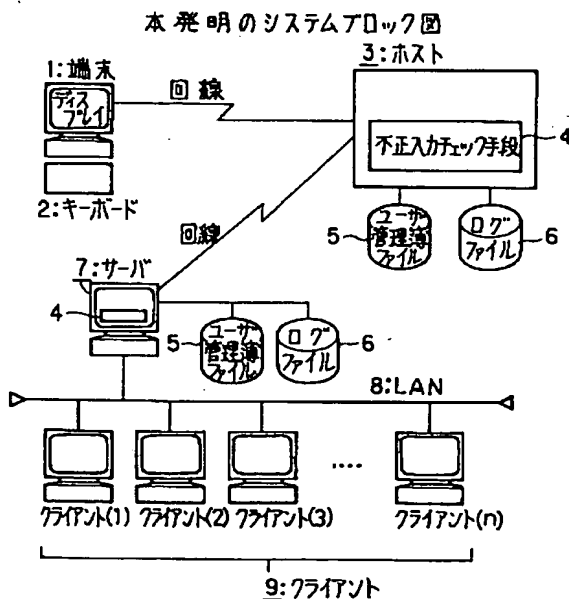
【図4】本発明の動作説明フローチャート(その2)である。

【図5】本発明の表示例である。

【符号の説明】

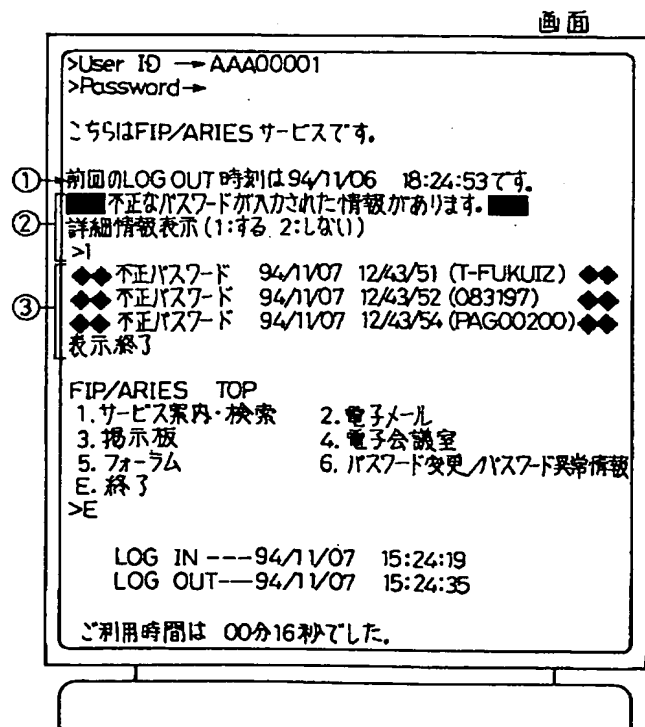
- 1: 端末
- 2: キーボード
- 3: ホスト
- 4: 不正入力チェック手段
- 5: ユーザ管理簿ファイル
- 6: ログファイル
- 7: サーバ
- 8: LAN
- 9: クライアント

【図1】



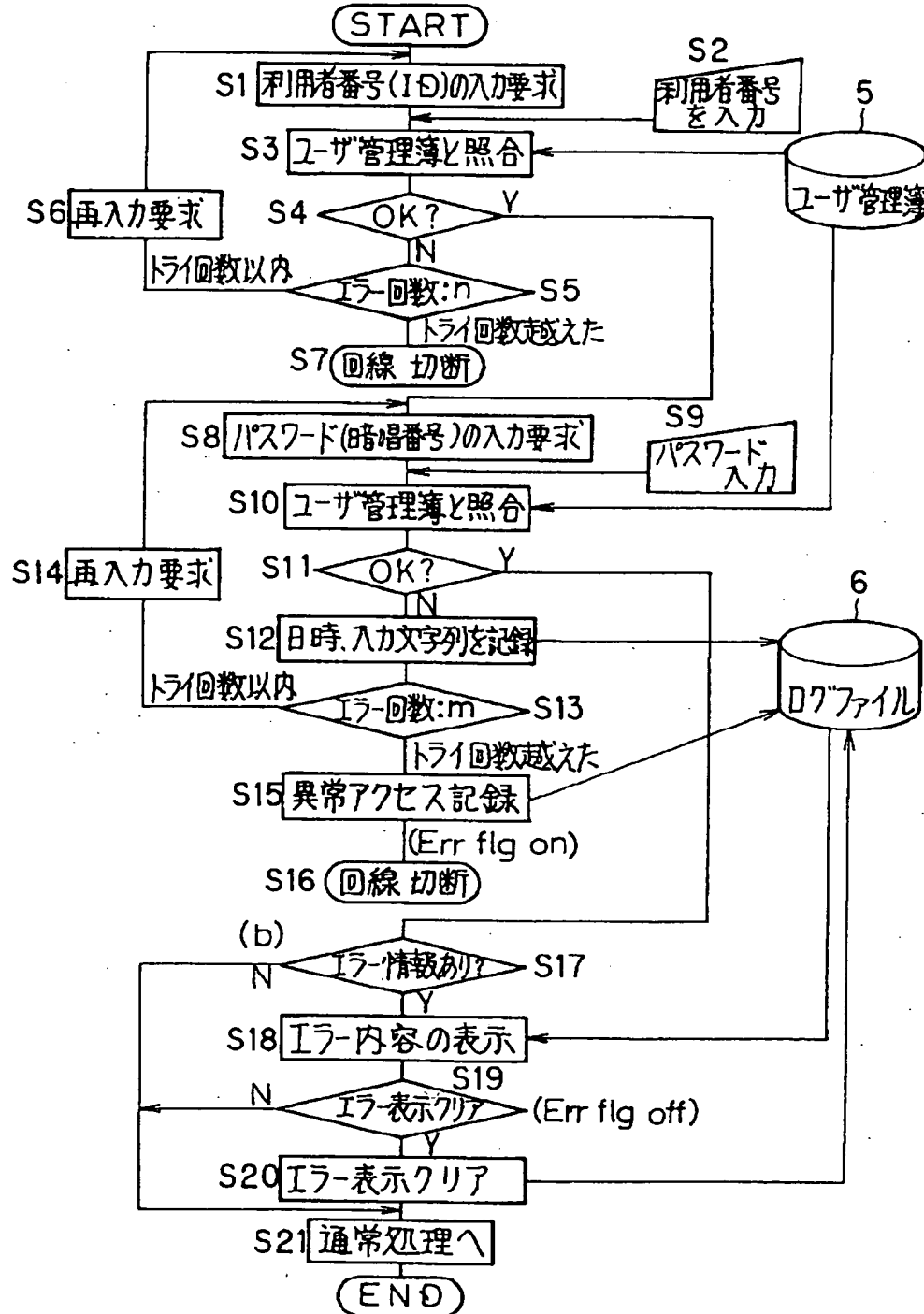
【図5】

本発明の表示例(パスワード入力エラー情報表示例)



【図2】

本発明の動作説明フローチャート(その1)



【図3】

本発明のファイル例

5:ユーザ管理簿ファイル

ID番号	パスワード		異常	ログ位置
AAA00001	T-FUKUJ		E	000001
AAA00002	082197		N	

6:ログファイル

000001							
日付け	時刻	1 回	時刻	2 回	時刻	3 回	続き
94/11/07	12:43:51	T-FUKUJZ	12:43:52	083197	12:43:54	PAG00200	00000

【図4】

本発明の動作説明フローチャート(その2)

